Amendments to the Claims:

A listing of the entire set of pending claims (including amendments to the claims, if any) is submitted herewith per 37 CFR 1.121. This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (Cancelled)

2. (Cancelled)

3. (New) A method for detecting malicious code patterns, the method comprising:

determining whether the values of tokens in two sentences of program code have the same value at the time of execution by one of:

(a) determining if both of the tokens in the two sentences are constants and if said determination is true, further determining whether relevant token character strings are identical to each other;

(b) determining if one of the tokens in the two sentences is a constant and the other token is a variable, and if said determination is true, further determining whether the relevant token character strings are identical to each other after the variable is substituted for the constant;

(c) determining if both of the tokens in the two sentences are variables and have the same name and range, and if said determination is true, further determining whether there are definitions of the relevant variables in a control flow from a preceding one of the two sentences to a following one thereof and if said determination is true, detecting said malicious code pattern;

(d) determining if both of the two tokens of the two sentences are variables but do not have the same name and range, and if said determination is true, further determining whether there are definitions of the relevant variables in a control flow from a

PATENT
Attorney Docket: 587-35

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT(S):	Hong, Man-Pyo	GROUP:	2136
SERIAL NO.:	10/799,527	EXAMINER:	Fikremariam Yalew
FILED:	March 12, 2004	Dated:	September 24, 2007

FOR: METHOD FOR DETECTING MALICIOUS CODE PATTERNS IN CONSIDERATION OF CONTROL AND DATA FLOWS

Mail Stop: AMENDMENTl
Commissioner for Patents
PO Box 1450
Alexandria, VA 22313

AMENDMENT UNDER 37 C.F.R. §1.111

Sir:

In response to the Non-Final Office Action of April 23, 2007, please amend the above identified application as follows:

Amendments to the claims are reflected in the listing of claims which begins on page 2 of this paper.

Remarks/Arguments begin on page 5 of this paper.

Certification under 37 C.F.R. §1.8

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail, postpaid in an envelope, addressed to: Mail Stop: AMENDMENT, Commissioner for Patents, PO Box 1450, Alexandria VA 22313-1450 on the date indicated below.

Dated: September 24, 2007

George M. Kaplan

Amendments to the Claims:

A listing of the entire set of pending claims (including amendments to the claims, if any) is submitted herewith per 37 CFR 1.121. This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (Cancelled)

2. (Cancelled)

3. (New) A method for detecting malicious code patterns, the method comprising:

determining whether the values of tokens in two sentences of program code have the same value at the time of execution by one of:

(a) determining if both of the tokens in the two sentences are constants and if said determination is true, further determining whether relevant token character strings are identical to each other;

(b) determining if one of the tokens in the two sentences is a constant and the other token is a variable, and if said determination is true, further determining whether the relevant token character strings are identical to each other after the variable is substituted for the constant;

(c) determining if both of the tokens in the two sentences are variables and have the same name and range, and if said determination is true, further determining whether there are definitions of the relevant variables in a control flow from a preceding one of the two sentences to a following one thereof and if said determination is true, detecting said malicious code pattern;

(d) determining if both of the two tokens of the two sentences are variables but do not have the same name and range, and if said determination is true, further determining whether there are definitions of the relevant variables in a control flow from a

preceding one of the two sentences to a following one thereof after the relevant variables are substituted for the original variables and if said further determination is true, detecting said malicious code pattern.

4. (New) The method of claim 2, wherein said determining step (d) of determining whether there are definitions of the relevant variables in a control flow from a preceding one of the two sentences to a following one thereof after the relevant variables are substituted for the original variables, further comprises performing a copy propagation to substitute relevant variables for original variables.

5. (New) The method of claim 4, wherein said copy propagation reduces the number of copies by finding a variable which will always have a specific constant value upon execution of a program and performing substitution through a copy sentence in the form of "x=y".

6. (New) The method of claim 3, wherein the copy propagation is performed via a data flow analysis in a created control graph to create a modified control graph.

7. (New) The method of claim 1, wherein said determining step (b) of determining whether there are definitions of the relevant variables in a control flow from a preceding one of the two sentences to a following one thereof further comprises performing a constant propagation to substitute relevant variables for original variables.

8. (New) The method of claim 7, wherein said constant propagation finds a variable or formula that will always have a specific constant value upon execution of a program.

9. (New) The method of claim 7, wherein the constant propagation is performed via a data flow analysis in a created control graph to create a modified control graph.